

RECEIVED
CENTRAL FAX CENTER

JUL 31 2006

CLAIMS

1. (Previously presented) A method comprising:

broadcasting a synchronization signal from a wireless access point device indicating one of a plurality of modes of operation for the access point, the plurality of modes of operation including a private mode of operation for authorized devices and a public mode of operation for authorized or non-authorized devices;

broadcasting available public network services if the mode of operation is the public mode of operation;

receiving a request for establishment of a connection from a non-authorized mobile device in response to the broadcast of a synchronization signal for the public mode of operation; and

establishing a connection between the non-authorized mobile device and the access point device;

wherein establishing a connection in the private mode comprises use of a secure authentication process, and wherein establishing a connection in the public mode comprises use of a registration process.

2. (Previously presented) The method of claim 1 further comprising:

receiving a request from the non-authorized mobile device for access to a selected network service of the available network services; and

allowing the non-authorized mobile device access to the selected network service.

3. (Previously presented) The method of claim 1, wherein the available network services include free public network services.

Attorney Docket No.: 42390P11398
Application No.: 10/090,136

-2-

4. (Previously presented) The method of claim 1, wherein the available network services include pay-per-use public network services.
5. (Original) The method of claim 4 further comprising:
providing a form of payment for a pay-per-use network service.
6. (Original) The method of claim 5 wherein the form of payment is a credit card number.
7. (Original) The method of claim 5 wherein the form of payment is a prepaid payment number.
8. (Original) The method of claim 5 further comprising:
providing a secure transmission of information between the non-authorized mobile device and the access point device.
9. (Original) The method of claim 5 further comprising:
sending payment information from the non-authorized mobile device to the access point device wirelessly.
10. (Original) The method of claim 5 further comprising:
validating the payment information provided by the non-authorized mobile device; and
providing the validation results to the non-authorized mobile device.
11. (Previously presented) The method of claim 10 further comprising:

establishing a connection between the non-authorized mobile device and a selected network service only if payment validation is successful.

12. (Previously presented) The method of claim 11 further comprising:
if a payment for the non-authorized mobile device expires, disconnecting the non-authorized mobile device from a selected network service of the available network services.
13. (Previously presented) The method of claim 1 further comprising:
performing data exchanges between the non-authorized mobile device and a selected network service of the available network services through the access point.
14. (Original) The method of claim 1 further comprising:
disconnecting the non-authorized mobile device from the access point device to terminate access to the available network services.
15. (Previously presented) The method of claim 1 wherein the establishment of the connection uses an authentication procedure provided in the Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification or its supplements.
16. (Previously presented) A machine-readable medium having one or more instructions for enabling a non-authorized user to wirelessly access a number of network services, which when executed by a processor, causes the processor to perform operations comprising:
wirelessly transmitting a synchronization signal indicating one of a plurality of modes of operation for an access point, the plurality of modes of operation including a

private mode of operation for authorized devices and a public mode of operation for authorized or non-authorized devices;

wirelessly transmitting available network services if the mode of operation is the public mode of operation;

receiving a request for connection establishment from a non-authorized user in response to the transmission of a synchronization signal for the public mode of operation;

establishing a connection with the non-authorized user;

receiving a request for access to a selected network service, from among the available network services, by the non-authorized user; and

providing the non-authorized user access to the selected network service;

wherein establishing a connection in the private mode comprises use of authentication and association handshakes, and wherein establishing a connection in the public mode comprises use of a registration process.

17. (Original) The machine-readable medium of claim 16 further comprising:

requesting a form of payment from the non-authorized user for access to pay-per-use network services.

18. (Original) The machine-readable medium of claim 17 further comprising:

validating the payment information provided by the non-authorized user.

19. (Previously presented) The machine-readable medium of claim 18 further comprising:

if payment from the non-authorized mobile device expires, disconnecting the non-authorized mobile device from the selected network service.

20. (Previously presented) The machine-readable medium of claim 16 further comprising:

performing data exchanges between the non-authorized user and the selected network service.

21. (Previously presented) An apparatus comprising:

a transceiver port for wirelessly communicating with mobile devices;

a network communications port communicatively coupled to the transceiver port, the network communications port for coupling to a network; and

a control unit coupled to the transceiver port and the network communications port, the control unit configured to control access from the transceiver port to the network communications port and provide at least two modes of operation, a first mode of operation to provide authorized mobile devices private access to the network communications port, and a second mode of operation to provide authorized and non-authorized mobile devices public access to the network communications port

wherein the control unit is to use the transceiver port to broadcast a synchronization signal indicating one of the modes of operation and, for the second mode of operation, available network services, and to receive a response from an unauthorized mobile device in response to the broadcast of the synchronization signal; and

wherein the control unit is to establish a connection in the private mode through use of authentication and association handshakes, and to establish a connection in the public through use of a registration process.

22. (Original) The apparatus of claim 21 wherein any one of the operation modes can be dynamically enabled or disabled.

Attorney Docket No.: 42390P11398
Application No.: 10/090,136

-6-

23. (Original) The apparatus of claim 21 wherein in the first mode of operation a specific authentication process is requested from the mobile devices to obtain full network access over the network communications port and in the second mode of operation no specific authentication process is requested from the mobile devices to obtain certain network access over the network communications port.

24. (Original) The apparatus of claim 21 wherein the second mode of operation allows the non-authorized mobile devices to obtain public network access through the network communication port.

25. (Original) The apparatus of claim 21 wherein the control unit is configured to provide secure services to both authorized and non-authorized mobile devices.

26. (Previously presented) The apparatus of claim 21 wherein the control unit is configured to provide data exchange to both authorized and non-authorized mobile devices utilizing an authorization process provided in the Electrical and Electronics Engineers (IEEE) 802.11 Standard or its supplements.

27. (Original) The apparatus of claim 21 wherein the control unit is configured to provide a third mode of operation, the third mode of operation provides authorized mobile devices access to the network communications port and non-authorized mobile devices limited access to the network communications port simultaneously.

28. (Previously presented) The method of claim 1, wherein the private mode of operation includes a secure service as specified in the Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification or its supplements.

29. (Previously presented) The method of claim 1, wherein the plurality of modes of operation includes a simultaneous mode of operation, the simultaneous mode of operation providing authorized mobile devices access to private network services and authorized or non-authorized mobile devices access to public network services simultaneously via the access point device.

30. (Previously presented) The machine-readable medium of claim 16, wherein the private mode of operation includes a secure service as specified in the Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification or its supplements.

31. (Previously presented) The machine-readable medium of claim 16, wherein the plurality of modes of operation includes a simultaneous mode of operation, the simultaneous mode of operation providing authorized mobile devices access to private network services and authorized or non-authorized mobile devices access to public network services simultaneously via the access point.

32. (Previously presented) The method of claim 15, wherein:
the establishment of a connection in the private mode comprises use of Secure Service procedures as specified in IEEE Standard 802.11 Specification or its supplements; and
the establishment of a connection in the public mode comprises use of Open System procedures as specified in IEEE Standard 802.11 Specification or its supplements.

33. (Previously presented) The machine-readable medium of claim 16, wherein:

the establishment of a connection in the private mode comprises use of Secure Service procedures as specified in the Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification or its supplements; and the establishment of a connection in the public mode comprises use of Open System procedures as specified in the IEEE Standard 802.11 Specification or its supplements.

34. (Previously presented) The apparatus of claim 26, wherein the control unit is configured to:

establish a connection in the private mode through use of Secure Service procedures as specified in IEEE Standard 802.11 Specification or its supplements; and establish a connection in the public mode through use of Open System procedures as specified in IEEE Standard 802.11 Specification or its supplements.